WHAT IS CLAIMED IS:

1. A storage apparatus for processing a command transmitted by a host computer connected to said storage apparatus by a network, said storage apparatus comprising:

a storage unit for storing data to be processed in accordance with said command;

a memory for holding an access management table for storing first information on identification of said host computer;

a first determination means for determining whether or not a frame of a login request transmitted by said host computer includes second information on identification of said host computer;

a request means for transmitting a request to a source address specified in the frame of the login request in order to request said host computer to transmit the first information on identification of said host computer in a case where the determination result output by said first determination means indicates that the frame of the login request does not include the desired second information; and

a second determination means for carrying out a determination process on the first information transmitted by said host computer in response to the request issued by

said request means by examination of said access management table;

wherein a decision as to whether or not to approve the login request is made in accordance with the determination result output by said second determination means.

2. A storage apparatus according to claim 1 wherein an access is made to said storage unit by adoption of an iSCSI protocol.

3. A storage apparatus according to claim 1 wherein the first information stored in said access management table is an MAC address of an interface with an IP network through which said host computer is connected to said storage apparatus.

4. A storage apparatus according to claim 1 wherein said storage apparatus further having an SNMP manager for monitoring an apparatus connected to said IP network, and wherein said SNMP manager transmits a frame, which is used for requesting said host computer to transmit the first information, as an SNMP request for requesting said host computer to transmit an MIB of an interface related to said host computer.

5. A storage apparatus according to claim 1, further comprising a console used for changing a content of said access management table.

6. A storage apparatus according to claim 1 wherein, if the determination result produced by said second determination means indicates that the first information for identifying said host computer is not stored in said access management table, a content of said login request is stored in said memory as log data.

7. A storage apparatus according to claim 3 wherein, if the determination result produced by said second determination means indicates that the first information for identifying said host computer has been stored in said access management table, a source IP address of the login request is stored in said access management table, being associated with said information for identifying said host computer.

8. A storage apparatus according to claim 3 wherein:

said access management table is used for cataloging a MAC address and an identification code for identifying a logical unit (LU) accessible to a host computer having an IP-network interface identified by the MAC address; and

prior to processing of a command received from said host computer, an access requested by the command is examined to determine whether or not the access is an access to an accessible logical unit and the command is processed only if the access is found out to be an access to an accessible logical unit.

9. A storage apparatus according to claim 3 wherein said access management table is used for storing an IP address assigned to a host computer having an IP-network interface identified by a MAC address as an address associated with the MAC address.

10. An access control management method for managing an access permit for an access request transmitted by an external apparatus to a storage apparatus by way of a network, said access control management method comprising the steps of:

receiving a frame of a login request from said external apparatus in said storage apparatus;

determining whether or not the received frame includes second information for identifying said external apparatus in a first determination process;

requesting acquisition of first information for identifying said external apparatus from said external apparatus in a case where a result of said first determination process indicates that the frame does not include the second information;

checking said acquired first information in a second determination process in order to determine whether or not an access permit should be given to said external apparatus; and

approving an access request made by said external

apparatus as a request for an access to said storage apparatus in a case where a result of said second determination process indicates that an access permit should be given to said external apparatus.

11. An access control management method according to claim 10 wherein a MAC address is used as the first information, and an IP address is used as the second information.

12. An access control management method according to claim 10, further comprising the step of preparing a table, which is used for cataloging first information for identifying an external apparatus allowed to make accesses to said storage apparatus;

wherein, in said second determination process, first information acquired from an external apparatus is checked by referencing said table in determination of whether or not an access permit should be given to said external apparatus.

13. An access control management method according to claim 10, further comprising the step of storing information on a frame of a received login request in a memory as log data in case a result of said first determination process indicates that said frame does not include said second information or a result of said second determination process indicates that an access permit

should not be given to said external apparatus.

14. An access control management method according to claim 10 wherein, at said step of requesting acquisition of first information for identifying an external apparatus from said external apparatus, an SNMP manager for monitoring an apparatus connected to said IP network requests said external apparatus to transmit the first information.

15. An access control management method according to claim 10 wherein, at said step of requesting acquisition of first information for identifying an external apparatus from said external apparatus, a MAC address is obtained from said external apparatus by adoption of a protocol based on an iSCSI text mode negotiation.

16. An access control management method according to claim 15, further comprising the steps of:

defining a plurality of logical units (LUs) in said storage apparatus;

preparing an access management table for storing a MAC address and an identification code for identifying one of said logical units, which is accessible to an external apparatus having an IP-network interface identified by said MAC address; and

determining whether or not an access requested by a command transmitted by an external apparatus is an access

to a specific one of said logical units, which has an

identification code cataloged in advance in said access

management table, with regard to processing of said command

in a third determination process after said second

determination process;

wherein said command is processed if a result of

said third determination process indicates that said access

requested by said command is an access to said specific

accessible logical unit.

17. An access control management method for managing

access permits for accesses made by a first apparatus as

accesses to a second apparatus connected to said first

apparatus by a network, said access control management

method comprising the steps of:

acquiring predetermined first information from said

first apparatus serving as an initiator of a communication

in a case where said communication is determined to be

unimplementable through said network in a first check mode

of determining whether or not an access made by said first

apparatus as an access to said second apparatus is an

access made through said network by checking second

information transmitted from said first apparatus to said

second apparatus; and

processing a command transmitted by said first

apparatus to said second apparatus if an access requested

by said command is permitted in a second check mode of determining whether or not an access made by said first apparatus as an access to said second apparatus is permitted by checking said first information acquired from said first apparatus.

18. An access control management method according to claim 17 wherein:

said first apparatus is a host computer;

said second apparatus is a storage apparatus including a plurality of defined logical units, and processing a command by adoption of an iSCSI protocol;

said first information is a MAC address; and

said second information is an IP address included in a frame transmitted by said first apparatus to said second apparatus.

19. An access control management method according to claim 17, further comprising the step of connecting said storage apparatus comprising an iSCSI layer, a TCP layer, an IP layer and a datalink layer with an IP network.

20. A command-processing method for carrying out a communication between a first apparatus having an iSCSI initiator and a second apparatus having an iSCSI target through an IP network, said command-processing method comprising the steps of:

receiving a frame of a login request made by said

first apparatus in said second apparatus;

checking whether or not said frame includes first predetermined information for identifying said first apparatus;

issuing a request from said second apparatus for acquisition of second predetermined information for identifying said first apparatus from said first apparatus in a case where said frame does not include said first predetermined information;

checking whether or not an access made by said first apparatus is to be permitted by examination of said second predetermined information transmitted by said first apparatus to said second apparatus; and

processing a command transmitted by said first apparatus to said second apparatus in said iSCSI target of said second apparatus in a case where a result of checking indicates that an access made by said first apparatus as an access to said second apparatus is permitted.

21. A command-processing method according to claim 20 wherein, as said second predetermined information, a MAC address is acquired by a communication between an SNMP agent employed in said first apparatus and an SNMP manager employed in said second apparatus.

22. A storage apparatus for executing a command received from a host computer connected to said storage

apparatus by an IP network, said storage apparatus comprising:

a storage unit for storing data to be processed by execution of said command;

a memory for holding an access management table for storing first information on identification of said host computer; and

a processing unit for processing a request received from said host computer;

wherein said processing unit:

carries out a first determination process to determine whether or not a frame of a login request received from said host computer includes second information on identification of said host computer;

transmits a request to a source address specified in said frame of said login request in order to request said host computer to transmit first information on identification of said host computer, and carries out a second determination process on first information transmitted by said host computer in response to said request by examination of said access management table in a case where a determination result output by said first determination process indicates that said frame of said login request does not include desired second information; and

makes a decision as to whether or not to approve said login request in accordance with a determination result output by said second determination process.